Paper Number 2004-01-037

ATTRIBUTES OF A MANAGERIAL AND ORGANIZATIONAL INFRASTRUCTURE TO ENABLE EFFECTIVE SAFETY PROGRAMS

Stuart D. Hann[1] and Scott Jackson[2]
Associate Technical Fellows, System Safety[1] & Systems Engineering[2]
The Boeing Company
Long Beach, California

Extensive research shows that for a system safety program to be effective, it must exist within an *organizational and managerial infrastructure* that contains *specific characteristics and attributes* that will enable it to meet its objectives. If it does not, even the best system safety effort will fail, and there are multiple examples of this occurring. This paper uses that research and additional work by the authors to present a coherent and useful arrangement of these *characteristics and attributes.* By presenting the attributes' *observable features* we show how these safety-enabling attributes can be confidently applied to any organization and managerial infrastructure. While these attributes are not a guarantee that a system safety program will be effective, they provide the means to assure that any system safety program will have an opportunity to perform at its best without being compromised by an inappropriate infrastructure. Case studies are cited and correlated to specific attributes which, if applied, would have mitigated the probability of a catastrophic occurrence. The opinions and conclusions in this paper are those of the authors and do not necessarily reflect the views of The Boeing Company.

Introduction

In an earlier paper (Jackson, 1991) showed that when an organization is viewed as a system, systems engineering methodology could be applied to derive the attributes of that organization that would enable safe and successful systems. Based on extensive research, the root causes of systems that caused accidents were used to derive preventive, qualitative *characteristics* and the objective *attributes* that enable them. Fostering these *preventive characteristics* in an organiza-tional and managerial infrastructure will reduce or eliminate the root causes and thus enable safety programs. In the context of this paper, managerial and organizational *attributes* are the equivalent of design features, namely, observable features of the managerial and organizational infrastructure that manifest the preventive characteristics. These features may include specific organizational relation-ships, existing organizational entities, existing and demonstrated programs or processes, or documentation, such as managerial directives. While much of the past research has been performed by experts in such fields as sociology and psychology, the objective of this paper is to bring the results of that re-search together in a systems engineering and safety program context to define the characteristics and observable attributes of a managerial and organiza-tional system that will enable safe, successful products to be delivered.

(Reason, 1991) emphasizes that not all accidents have organizational roots. [Note: Reason uses the term *organizational* to include both the organizational structural aspects and the managerial aspects referred to in this paper.] Reason even gives examples in which well-planned programs resulted in major accidents and other examples in which badly planned programs were successful. Nevertheless the researchers have identified the positive characteristics and the resulting attributes that will avoid the root causes and thus enable effective safety programs. This paper expands on this research to synthesize a unified set of characteristics and attributes.

Case Histories, Root Causes, and Preventive Characteristics

Previous investigators, in particular (Reason, 1997) and (Paté-Cornell, 1990) have identified numerous root causes of programs that caused accidents. (Jackson, 1991) has provided short summaries of the major case histories; these are summarized here in brief statements. In this paper we have combined the root causes into six major categories; the other root causes are subsets of these six. The discussion of each case history and root cause is followed by a correlated preventive-characteristics statement. When the noted preventive characteristics are present, they eliminate the accident root causes. Therefore, an organizational and managerial infrastructure which possesses these characteristics will support and enable effective safety efforts. Figure 1 shows which of the root causes each positive characteristic addresses, along with the observable attributes that are manifested when each characteristic is present. This figure, the characteristics, and the attributes are based upon the research and the additional work by the authors.

The six root-cause categories are as follows:

1. Lax Regulation. Failure in regulation can manifest itself in three ways. First, the developer or operator may be uncooperative with the regulatory agency. Secondly, the regulatory agency may be negligent in their duties or completely absent. Finally, the regulatory agency may be too close to the developer or operator to exercise effective oversight.

According to (Hughes, 1997), the US Coast Guard had adopted a passive attitude towards the regulation of explosive materials with respect to the Texas City

[Texas] disaster of 1947 in which approximately 600 people were killed when a ship exploded in the harbor. The Coast Guard had not been checking any ships unless they were notified in advance, which was infrequent. As a result of this passive approach, no one present knew of the explosive nature of the cargo until it exploded.

The second example is given by (Reason, 1997) regarding the London Underground (subway) fire in which the lines between the operator and the regulator became so blurred that very little inspection was performed. The result was a fire in a stairwell in which many people were killed.

The root causes of accidents involving lax regulation involve factors pertaining to the developer, the operators, and the regulators themselves. Hence, any requirements involving regulation would necessarily would need to be laid on all three entities.

Preventive Characteristics: Organizations shall maintain relationships with their regulatory agencies which allow those agencies to achieve their objectives. First of all, a policy of engagement and cooperation shall be maintained. Secondly, regulatory agencies shall demonstrate control over those areas for which they are responsible. Third, the regulatory agencies and organizations which they oversee shall maintain a policy of independence.

2. Lack of Clear Line of Safety Decisions. In many organizations the responsibility for safety decisions is blurred both vertically and horizontally. This blurring leads to lacks of initiative and assertiveness about safety issues due to lack of clarity of who is responsible; inaction results. In a well-structured organization, management directives will make it clear that safety decisions will be made at the lowest possible level and that the persons at that level have the expertise to make the proper decisions (see Lack of Expertise, 6, below). Another aspect of safety decisions is that they will be *independent*, that is to say, safety-related decisions will involve at least two separate lines of management. For example, the two functions of product assembly and inspection will be vested in separate chains of management, as will the product safety and design groups.

Preventive Characteristic: An organization shall maintain a policy of clear and independent paths of safety decisions made at the lowest level possible. Persons with decision making authority shall have the expertise to make proper safety decisions.

3. Communication Failure and Loss of Information. This root cause includes the lack of technical and non-technical information when it is critical information needed to accomplish the mission safely. Often this information travels through the hands and computers of many people and often across organizational boundaries. No example is more poignant that that of Jesica Santillan (CBS, 2003) who died when the heart transfer system failed to match her blood type with that of the donor heart when she was having a transplant. This information path is called an *information thread* and, in this case, it was a faulty thread.

According to (Reason, 1997) and (Paté-Cornell, 1990), the North Sea oil disaster was an example of communications failure. An information thread was broken when a maintenance crew failed to tell the next shift that a pump had not been turned off. The result was a fire in which hundreds perished.

Preventive Characteristics: An organization shall maintain clear paths of communications from the points of view of both person-to-person information transfer, and the technical information and data itself, via whatever media are used and through whatever organizational boundaries are crossed. Adequate redundancy shall be built into the system to ensure the reliable transmission of safety-critical information and data, and the organization shall be structured to ensure the directness of such transmissions. Information and data transmission across internal and external organizational boundaries shall be similarly ensured.

4. Unclear Risks. The London Underground fire (Reason, 1997) stands also an example of the failure to assess risks properly. The primary risk focused on by the operators and regulators was the risk of train collisions. This focus resulted in the failure to recognize that there were other risks, such as the risk of fires in the station, which could and did have serious consequences.

Preventive Characteristics: An organization shall maintain a broad-focused and candid risk assessment and management program to ensure that technical, schedule and cost risks are identified, analyzed, and managed. The risk management program shall ensure that risks both under the control of and external to the organization are addressed. Mitigation steps identified shall be incorporated into program planning and executed.

5. Funding, Scope, and Schedule Pressures. The essence of program management is balancing the needs of the program against outside pressures. Cost and schedule pressures are familiar to everyone, and they are immediate. Safety, and the managerial and organizational infrastructure attributes that support it, seem abstract and distant in comparison to cost and schedule, and the effects of their neglect are delayed. This puts extra responsibility on program managers to resist the pressure to compromise safety in favor of more immediate concerns. According to (Reason, 1997), Valeri Legasof, the principal investigator at Chernobyl, asserted that the accident was "...the summit of the incorrect running of the economy which had been going on in our country for many years."

Preventive Characteristic: A safety organization must have adequate funding, scope, and schedule to

achieve its objectives. Authority must be delegated to the appropriate safety segment of the organization to determine the amount of funding that is appropriate, the needed scope of the safety effort, and the realizable schedule. That authority's assessment shall be binding.

6. Lack of Expertise. The Texas City explosion is also a good example of the lack of expertise, in this case, of the captain of the ship with his cargo. In a misguided action, according to (Hughes, 1997), the captain ordered the hatches to be closed to protect the rest of the cargo from a fire. This action had the effect of increasing the pressure and temperature and thus precipitating a larger explosion.

Preventive Characteristics: An organization shall ensure that all personnel have the expertise to take the required actions in the event of safety-related situations. Both management and non-management personnel shall be trained in these skills. Training shall include the recognition of safety-critical situations and the appropriate actions to take in these situations, including when immediate action is needed.

Observable Attributes Manifested by the Preventive Characteristics

The list below constitutes the managerial and organizational infrastructure attributes manifested from the preventive characteristics which create successful systems and enable effective safety programs (see Figure 1). These observable attributes are the features, processes, and structures of an organization and its management, separate from the individuals within that organization, that influence the effectiveness of system safety for better or worse. In order to be usefully applied, these attributes must be have observable features which permit their management to ensure the preventive characteristics are present. Documents, organizational structures, and existing program elements are attributes, and they have observable features.

a. Safety Priority. For each site or program, the program manager's directive (the attribute) makes clear the at least equal, if not superior, priority of system safety and safety-related decisions in relation to other program priorities. Consistent adherence to this priority contributes to the development of a safety culture by making clear to all the reality of the policy of safety's priority. This directive will be widely disseminated, and will inform all members of the site or program of the priority of safety and the safety significance of the safety-enabling managerial and organizational aspects of their program. Provisions of this directive will be highlighted in training programs for managers and engineers at all levels to help drive this home.

b. Decision Making. A policy is established to ensure that safety-related decisions are made at the lowest possible level by people who have the expertise to make them, and that they are made involving lines of safety authority separate from the normal line function responsible for them. Inspection of the organization charts shall demonstrate that the structure of the organization enables this policy to be followed.

c. Regulatory Relations. The organization establishes a policy of engagement and cooperation with all regulatory agencies. The organization maintains a policy of independence from regulatory agencies such that an organization position on any given safety issue is arrived at separately from that of the regulatory agency.

d. Corrective Action System. A corrective action system is established with the authority to make the changes necessary to ensure system safety and maintenance of the organizational and managerial attributes.

e. Safety Oversight. Program managers publish directives delegating responsibility for site and/or program system safety to the System Safety organization. The System Safety lead creates and maintains internal procedures for implementing positive managerial and organizational attributes to enable safety.

f. Independent Reviews. An independent review or audit process is established to assess the health and effectiveness of safety processes and their implementations on each site, program, and associated organization. Independent assessment reviews ensure the independence and effectiveness of each program's assessment and management of safety issues. Independent reviews also facilitate the acceptance of the safety program and the product's safety by outside agencies. Independent assessors from organizations other than the one being evaluated are invited to participate in the audit program. The independent assessors can review, for example, whether the budget, schedule and scope of work are compatible with the program demands and whether the associated organizations are maintaining the positive managerial and organizational attributes. To be fully effective, the review teams are free to assess the program without being asked. In addition, they are free to re-port their findings to higher enterprise-level management if they feel their recommendations are not being followed. The necessary directives identified by this paper are the primary source of review criteria.

g.-j. Direct Communications and Feedback. Of all desirable attributes identified by the various investigators, communications is the most frequently mentioned. Effective safety communications are enabled in various ways. First, the placement of key managers, such as the System Safety lead, in a position directly reporting to the program manager

has a direct and positive effect on communications between them. A second element of a good safety communications system is a clear policy allowing any member of the organization to report safety issues. To implement this communications system fully, an anonymous reporting system must be established. Third, the program manager seeks feedback from safety evaluation teams, which are convened and dedicated to this purpose. Team responsibility includes initiating actions needing immediate response. The presence of non-advocate members on these teams is essential to achieve objectivity, a non-advocate member being a person who is not in the organization. Representatives from regulatory agencies are invited to be members of high-level safety-evaluation teams. The evaluation teams provide periodic summary reports to the program manager in which particular attention is paid to incidents and other escapes for which long-term corrective actions and process improvements need to be taken to ensure safety issue non-recurrence.

Fourth, the program manager establishes a policy of cooperation with regulatory agencies for communication on compliance with regulations. This policy specifies that all interactions between organization and regulatory agencies will be conducted with integrity and in an ethical, professional, and respectful manner.

Lastly, in addition to the organization-dependent communications, the safety enabling and preserving operation of any enterprise depends on the reliable flow of safety-critical information from sources to destinations. Sometimes this information has to pass through many nodes of the enterprise and sometimes it has to pass across organizational boundaries, for example, from a developer to a supplier. Sometimes this information is passed verbally, other times by paper, email, or fax, but whatever the means, when a multi-stage communication must occur, that is an *information thread*. An example of an information thread with safety-critical information is the blood type of a donated heart; this needs to be passed through multiple steps from the organ-providing organization to the hospital that must match it to the blood type of the patient. History shows such threads, and their failure, are notoriously troublesome and are a continuing source of communication breakdown. Clear, direct paths of communication, each explicitly and thoroughly examined for adequate integrity and redundancy, must be established and maintained for each safety-critical information thread.

k. Incentive System. As a visible means of demonstrating that reporting of safety conditions is encouraged, a recognition and rewards system is established. For example, a production person who reports repeated tags and the engineering person who resolves their repetition would both be recognized for their efforts. If there are cost and schedule goals bonus systems for executives and other personnel, equivalent bonus systems that reflect good accomplishment of the quality and safety of the product or program are also established. All management incentives and objectives will give equal emphasis to safety, and will not respond solely to cost and schedule goals.

l. Risk Analysis. A risk analysis and management process is used to ensure that all steps necessary to ensure a safe product or program have been taken. Risk processes typically focus on three types of risk: technical, schedule, and cost; assessment and management of all three are necessary to ensure safety. Technical risk analysis ensures that each component of the system meets its technical requirements and that compliance with those requirements has been verified by test, analysis, or other means. Schedule and cost risk analysis ensures that the program has adequate cost and schedule margin to meet its safety goals and challenges.

m. Funding, Schedule, and Scope Control. A frequent root cause of safety risk is inadequate funding. To counteract this, the program manager provides a directive that assigns System Safety the responsibility for determining the level of funding which is adequate to ensure product or program safety. Program Managers will retain their final approval of funding levels based on the System Safety determination but shall not compromise it.

In the same directive, System Safety is given the responsibility for determining schedule requirements to ensure system safety. Program managers have the responsibility for implementing the System Safety schedule based upon this determination.

Finally, the directive assigns System Safety the responsibility for determining the scope of the efforts needed to ensure the safety of the product or program. This responsibility goes beyond design aspects of the system and includes any program aspect that may affect safety, including specifically its organizational and managerial attributes. Thus, communications, reporting, evaluation, corrective actions, incentive programs, and training are explicitly included in this scope. Program managers have the responsibility for implementing the System Safety program within this determined scope.

The program will ensure sufficiently broad and deep participation with suppliers, partners, alliances, subsidiaries, affiliates, customers, regulatory agencies, and any other stakeholders that may be affected, or whose actions may affect safety. Those other organizations are required to comply with the provisions of the directive through their written agreements.

n. Training. The following attributes ensure that proper training is provided to inform all personnel regarding the priority and significance of safety, the managerial and organizational attributes enabling safety, and each person's role in maintaining these.

First, training regarding their responsibilities with respect to safety is mandatory for all employees and managers. This program familiarizes all members of the organization with the priority of safety, the principles and intents of the safety-enabling managerial and organizational attributes, their personal responsibilities to create and maintain these, and the effects on safety if these attributes are compromised. This training is annually refreshed to all personnel. Second, the System Safety lead provides needed content-revisions to the managerial and organizational safety training material based on escapes which were not covered by the existing training materials, and these revisions are incorporated prior to each annual training refresher. Third, this training program ensures that all members of each program know that safety problems are reportable, and that they are enabled and expected to report on them. Specific safety problem examples will include, but not be limited to, knowledge that reportable safety conditions are: (a) any specific safety design requirement that is not met by the system design implementation, (b) production procedures that may result in the failure of the system to perform as intended, (c) support procedures that may result in non-compliant conditions, (d) operational procedures that may result in non-compliant conditions or may be unsafe, (e) steps skipped or done inadequately at any phase of the program or product life cycle, due to schedule, cost, or other constraints or process failures, that may result in non-compliant conditions or may lead to unsafe conditions, and (f) non-compliant conditions that may result from inadequate training of or by other persons.

Conclusions

Even though organizational and managerial dynamics are in the realm of sociology or psychology, it is clear that the program organizational and managerial infrastructure is a system that must perform its functions properly to multiple, stringent requirements when safety is involved. If the characteristics and attributes of this infrastructure can be identified and controlled, then the effective safety functioning of this organizational and managerial system will be enabled. Research on this subject shows that such attributes can indeed be identified and described as they have been here, and that if these attributes are implemented, then the likelihood of major accidents will be reduced.

References

Hughes, Stephen, The Texas City Disaster, 1947, University of Texas Press, 1997

Jackson, Scott, Organizational Safety: A Systems Engineering Perspective, INCOSE Proceedings, 1991.

Paté-Cornell, Elizabeth, Organizational Aspects of Engineering System Safety: The Case of Offshore Platforms, Science, Vol. 250, 1990.

Reason, James, Managing the Risks of Organizational Accidents, Ashgate Publishing Limited, UK, 1997.